Arvados - Feature #16678

Default lifetime for tokens issued through login

08/10/2020 08:19 PM - Peter Amstutz

Status:	Resolved	**Start date:**	08/24/2020
Priority:	Normal	**Due date:**	
Assigned To:	Lucas Di Pentima	**% Done:**	100%
Category:	API	**Estimated time:**	0.00 hour
Target version:	2020-08-26 Sprint		

Description

Add a configuration where tokens issued through web login have a default lifetime. An expiration time of 8 or 12 hours implements a policy where users are required to log in again each day, and limits the amount of time an attacker could make use of a stolen token. The token is prevented from manipulating other tokens (i.e. getting other tokens or creating a new token without an expiration).

Document this feature in the admin section.

Subtasks:

Task # 16690: Review 16678-login-tokens-lifetime-config	**Resolved**

Related issues:

Related to Arvados Epics - Story #16520: GxP Qualification	**Resolved**	**08/01/2020**	**04/30/2021**

Associated revisions

Revision bd8bdd90 - 08/25/2020 06:00 PM - Lucas Di Pentima

Merge branch '16678-login-tokens-lifetime-config'
Closes #16678

Arvados-DCO-1.1-Signed-off-by: Lucas Di Pentima <lucas@di-pentima.com.ar>

History

#1 - 08/10/2020 08:19 PM - Peter Amstutz

- Category set to API

- Description updated

#2 - 08/10/2020 08:20 PM - Peter Amstutz

- Description updated

#3 - 08/10/2020 09:09 PM - Peter Amstutz

- Related to Story #16520: GxP Qualification added

#4 - 08/12/2020 02:24 PM - Peter Amstutz

- Target version set to 2020-08-26 Sprint

#5 - 08/12/2020 02:25 PM - Peter Amstutz

- Description updated

#6 - 08/12/2020 03:54 PM - Lucas Di Pentima

- Assigned To set to Lucas Di Pentima

#7 - 08/13/2020 07:06 PM - Lucas Di Pentima

- Status changed from New to In Progress

#8 - 08/19/2020 04:01 PM - Peter Amstutz

- Release set to 25

#9 - 08/24/2020 01:25 PM - Lucas Di Pentima

Updates at 00e16fb - branch 16678-login-tokens-lifetime-config

Test run: https://ci.arvados.org/job/developer-run-tests/2026/

- Sets new config knob Login.TokenLifetime that takes a Duration value that will be used to set the expires_at field on ApiClientAuthorization resources. Its default value is zero meaning that the feature is disabled.
  - Now that I see it with fresh eyes after the weekend, it may be more consistent to name it something like Login.TokenTTL
- On tokens created from a login flow:
  - Set the token expiration date if configured.
  - Set the is_trusted flag to false even if coming from trusted URLs (workbenches) to avoid the user to create new tokens.
- Adds rake tasks db:check_long_lived_tokens and db:fix_long_lived_tokens to allow the site admin to migrate from a previous token policy (eg: unexpiring tokens) to a more strict policy wrt to preexistent tokens.

Pending: Documentation

#10 - 08/24/2020 07:48 PM - Lucas Di Pentima

Documentation added at 46fefa537

#11 - 08/25/2020 05:46 PM - Peter Amstutz

I pushed some updates to the documentation at 3e38df9fabcbf421ef0b0aac2e82f92373c0e70f rest LGTM!

#12 - 08/25/2020 06:19 PM - Anonymous

- % Done changed from 0 to 100

- Status changed from In Progress to Resolved

Applied in changeset arvados|bd8bdd90055d61263eff5bdb9a953c57319aa83d.